

LDV/ZI 2010R00631

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA

v.

DANIEL SPITLER and
ANDREW AUERNHEIMER

:
:
:
:
:
:
:

CRIMINAL COMPLAINT

Mag. No. 11-4022 (CCC)

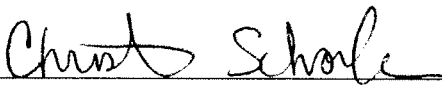
I, Christian Schorle, being duly sworn, state the following is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.



Christian Schorle, Special Agent,
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
January 13, 2011, at Newark, New Jersey



HONORABLE CLAIRE C. CECCHI
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Count 1

(Conspiracy to Access a Computer without Authorization)

From on or about June 2, 2010 through on or about June 11, 2010, in the District of New Jersey, and elsewhere defendants

DANIEL SPITLER and
ANDREW AUERNHEIMER

knowingly and intentionally conspired with each other and others to access a computer without authorization and to exceed authorized access, and thereby obtain information from a protected computer, namely the servers of AT&T, in furtherance of a criminal violation of the laws of the State of New Jersey, specifically, N.J.S.A. 2C:20-31, contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii), in violation of Title 18, United States Code, Section 371.

Count 2

(Fraud in Connection with Personal Information)

From on or about June 2, 2010 through on or about June 11, 2010, in the District of New Jersey, and elsewhere defendants

DANIEL SPITLER and
ANDREW AUERNHEIMER

knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons, including means of identification of thousands of New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to Title 18, United States Code, Section 1030(a)(2)(C), in violation of Title 18, United States Code, Section 1028(a)(7).

ATTACHMENT B

I, Christian Schorle, am a Special Agent with the Federal Bureau of Investigation. I have knowledge of the facts set forth below from my involvement in the investigation, a review of reports, and discussions with other law enforcement personnel. Any statements attributed to individuals are described in substance and in part.

1. Since in or about June 2010, the Federal Bureau of Investigation has been investigating a data breach at AT&T that resulted in the theft of personal information of approximately 120,000 AT&T customers, thousands of whom are New Jersey residents. That data breach and associated theft were perpetrated by Daniel Spitler (“defendant Spitler”) and Andrew Auernheimer (“defendant Auernheimer”) for the express purpose of causing monetary and reputational damage to AT&T and monetary and reputational benefits to the defendants.

A. The iPad and AT&T

2. At all times relevant to this Complaint:

a. The iPad, introduced to the market on or about January 27, 2010, was a device developed and marketed by Apple Computer, Inc. It was a touch-screen tablet computer, roughly the size of a magazine. The iPad allowed users to, among other things, access the Internet, send and receive electronic mail, view photographs and videos, read electronic books, word-process, and create spreadsheets and charts.

b. AT&T Communications, Inc. (“AT&T”) was an interexchange carrier and long distance telephone company headquartered in Bedminster, New Jersey. Among other things, AT&T provided certain iPad users with Internet connectivity via AT&T’s 3G wireless network.¹

c. AT&T offered two data plans for iPad 3G users: 250 MB of data per month for \$14.99 and 2 GB of data per month for \$25.² iPad 3G users who wished to subscribe to the AT&T 3G network had to register with AT&T. During the registration process, the user was required to provide, among other things, an e-mail address, billing address, and password.

d. At the time of registration, AT&T automatically linked the iPad 3G user’s e-mail address to the Integrated Circuit Card Identifier (“ICC-ID”) of the user’s iPad, which was

¹ Both Wi-Fi and the 3G wireless network were mechanisms by which users could access the Internet. For some iPad models, Internet connectivity was provided strictly over Wi-Fi, while others offered a combination of Wi-Fi and AT&T’s 3G wireless network.

² Until on or about June 7, 2010, AT&T also offered a third data plan, which allowed users unlimited access to data for \$29.99 per month.

a 19 to 20 digit number unique to every iPad (specifically, unique to the Subscriber Identity Module (“SIM”) card in the iPad). Accordingly, each time a user accessed the AT&T website, his ICC-ID was recognized and, in turn, his e-mail address was automatically populated, providing the user with speedier and more user-friendly access to the website.

e. The ICC-IDs and associated iPad 3G user e-mail addresses were not available to the public and were kept confidential by AT&T.

B. The Data Breach

3. Prior to mid-June 2010, when an iPad 3G communicated with AT&T’s website, its ICC-ID was automatically displayed in the Universal Resource Locator, or “URL,” of the AT&T website in plain text. Seeing this, and discovering that each ICC-ID was connected to an iPad 3G user e-mail address, hackers wrote a script termed the “iPad 3G Account Slurper” (the “Account Slurper”) and deployed it against AT&T’s servers. AT&T’s servers are protected computers as defined in Title 18, United States Code, Section 1030(e)(2).

4. The Account Slurper attacked AT&T’s servers for several days in early June 2010, and was designed to harvest as many ICC-ID/e-mail address pairings as possible. It worked as follows:

- a. The Account Slurper was designed to mimic the behavior of an iPad 3G so that AT&T’s servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the Account Slurper access to AT&T’s servers.
- b. Once deployed, the Account Slurper utilized a process known as a “brute force” attack – an iterative process used to obtain information from a computer system – against AT&T’s servers. Specifically, the Account Slurper randomly guessed at ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/e-mail pairing for a specific, identifiable iPad 3G user.

5. From on or about June 5, 2010 through on or about June 9, 2010, the Account Slurper attacked AT&T’s servers, gained unauthorized access to those servers, and ultimately stole for its hacker-authors approximately 120,000 ICC-ID/e-mail address pairings for iPad 3G customers. This was done without the authorization of AT&T, Apple, or any of the individual iPad 3G users.

C. Andrew Auernheimer and Goatse Security Take Credit for the Breach

6. On or about June 9, 2010, immediately following the theft, the hacker-authors of the Account Slurper provided the stolen e-mail addresses and ICC-IDs to the website Gawker

(<http://gawker.com>).³ Gawker proceeded to publish on its website the stolen information, albeit in redacted form, as well as an article concerning the breach (the “Gawker Article”).

7. The Gawker Article provided in relevant part:

A security breach has exposed iPad owners including dozens of CEOs, military officials, and top politicians. They – and every other buyer of the cellular-enabled tablet – could be vulnerable to spam marketing and malicious hacking. The breach . . . exposed the most exclusive email list on the planet, a collection of early-adopter iPad 3G subscribers that includes thousands of A-listers in finance, politics and media, from New York Times Co. CEO Janet Robinson to Diane Sawyer of ABC News to film mogul Harvey Weinstein to Mayor Michael Bloomberg. It even appears that White House Chief of Staff Rahm Emanuel’s information was compromised. It doesn’t stop there. According to the data we were given by the web security group that exploited vulnerabilities on the AT&T network, we believe 114,000 user accounts have been compromised, although it’s possible that confidential information about every iPad 3G owner in the U.S. has been exposed.

8. Under the heading, “Breach details: Who did it, and how,” the Gawker Article reported: “The [AT&T] subscriber data was obtained by a group calling itself Goatse Security.” The Article continued:

The group wrote a PHP script to automate the harvesting of data. Since a member of the group tells us the script was shared with third-parties prior to AT&T closing the security hole, it’s not known exactly whose hands the exploit fell into and what those people did with the names they obtained. A member tells us it’s likely many accounts beyond the 114,000 have been compromised.⁴

9. On the same day the Gawker Article appeared, June 9, 2010, a post was made to the LiveJournal weblog, <http://weev.livejournal.com>, which read: “Oh hey, my security consulting group just found a privacy breach at AT&T[.]”⁵ The post further linked to the Gawker Article and stated: “[T]his story has been broken for 15 minutes, twitter is blowing the fuck up,

³ Gawker is a website that advertises itself as providing “Gossip from Manhattan and the Beltway to Hollywood and the Valley.”

⁴ In fact, as noted above, information was stolen from approximately 120,000 accounts.

⁵ LiveJournal is a social networking website on which users can set up personal weblogs and post messages. Once a weblog has been created, only the user of that weblog can post messages and content on that weblog.

we are on the forntpage of google news and we are on drudge report (the big headline)[.]”⁶ The “User Profile” for the LiveJournal weblog, <http://weev.livejournal.com>, listed the user as “weev” with the name “Escher Auernheimer.”

10. On or about June 10, 2010, the website CNET published an article titled, “Hacker defends going public with AT&T’s iPad data breach (Q&A).” The article reported: “On Thursday, CNET talked to a key member of Goatse – Escher Auernheimer, also known as ‘Weev’ – about the group and what motivates them.” In the article, a question and answer dialog was presented, including the following:

Q: So, one of your members had an iPad and noticed this strange interaction with the AT&T Web site?

A: He used this AT&T security maintenance app. It was part of the normal user experience that tipped him off to something that would allow him to scrape this data.

Q: Then a script was written to do an automated brute force, right?

A: Correct.

11. More recently, on or about November 17, 2010, in an e-mail sent to an Assistant United States in the District of New Jersey, defendant Auernheimer again took credit for the data breach and associated theft of ICC-ID/e-mail address pairings, writing: “AT&T needs to be held accountable for their insecure infrastructure as a public utility and we must defend the rights of consumers, over the rights of shareholders. . . . I advise you to discuss this matter with your family, your friends, victims of crimes you have prosecuted, and your teachers for they are the people who would have been harmed had AT&T been allowed to silently bury their negligent endangerment of United States infrastructure.”

D. Goatse Security

12. Through their investigation, federal law enforcement officers have learned that Goatse Security is a loose association of Internet hackers and self-professed Internet “trolls.”⁷ Indeed, defendant Auernheimer has previously been public and outspoken about his trolling activities. For example:

⁶ All spelling and grammatical errors in this paragraph are per the original.

⁷ A “troll” is a person who intentionally, and without authorization, disrupts services and content on the Internet.

- a. In an August 3, 2008 interview with *The New York Times*, defendant Auernheimer admitted: “I hack, I ruin, I make piles of money. I make people afraid for their lives. Trolling is basically Internet eugenics. I want everyone off the Internet. Bloggers are filth. They need to be destroyed. Blogging gives the illusion of participation to a bunch of retards. . . . We need to put these people in the oven!”
- b. Likewise, in an interview with the website Corrupt in August 2008, defendant Auernheimer stated: “The security industry does not work against hackers. Security is a myth, there is no system that cannot be broken. . . . For the companies I’ve targeted, I’ve showed up at their parties and given some friendly greetings to bask in the looks of disgust and disdain. I take credit and responsibility for my actions.”
- c. Defendant Auernheimer also maintains a webpage at www.blip.tv, which is a website that, like YouTube, allows users to create and post videos. On his blip.tv page, Auernheimer posted several “sermons” in the guise of the “iProphet.” One such video was entitled “Sermon on Fear and The Men In Black/Direct Democracy.” During this video, Auernheimer stated: “Trolling can frequently have large economic repercussions as, as I learned, I learned when I trolled Amazon. I saw a one billion dollar change in their market capitalization. That’s the most monetary affection [sic] of a publicly traded stock that I’ve ever personally done. I mean, I’ve caused a more dramatic shift in price, but never market capitalization.” Auernheimer continued: “So a billion dollars changed hands as a result of my trolling, and I’m very, very glad to know that such insignificant things on the Internet can have drastic, far reaching effects.”

13. According to the Goatse Security website, the Goatse Security “Team” includes eight members, among whom are defendant Auernheimer and “JacksonBrown.” Through various investigative techniques, law enforcement officers have identified “JacksonBrown” as defendant Spitler.

14. The Goatse Security website describes defendant Auernheimer as having “[e]xtensive offensive web app vuln and business logic exploitation experience. Bash while drunk, perl while tripping, Ruby while living in SF SoMa. Representing antisecc, Bantown and Encyclopedia Dramatica. President of the GNAA.” Defendant Spitler is described as an “embedded and mobile devices engineer. PPC assembly. GNAA, obviously.” The Goatse Security website provides a hyperlink to the GNAA website.

15. The GNAA website states that “[t]his website is maintained by the GNAA, world-famous trolling organization.” The GNAA website provides hyperlinks to the Goatse Security website, as well as defendant Auernheimer’s LiveJournal weblog.

E. The Internet Relay Chats

16. On or about June 15, 2010, pursuant to a search warrant signed by the Honorable Erin L. Setser, U.S.M.J. in the Western District of Arkansas, law enforcement officers conducted a search of defendant Auernheimer's home, located in Fayetteville, Arkansas. During the execution of the search warrant, defendant Auernheimer agreed to speak with federal law enforcement officers and stated, among other things, that he and the other members of Goatse Security often communicated with one another using an online medium known as Internet Relay Chat, or "IRC."

17. Approximately one month after the search of defendant Auernheimer's home, a confidential source (the "CS") contacted federal law enforcement officers and stated, among other things, that the CS routinely monitored "#dominion," one of the IRC channels used by Goatse Security members to communicate with one another. The CS also provided law enforcement officers with chat logs from the "#dominion" channel from on or about June 2, 2010 through on or about June 11, 2010. Extending over 150 pages, those chat logs conclusively demonstrate that defendants Spitler and Auernheimer were responsible for the data breach and conducted the breach to simultaneously damage AT&T and promote themselves and Goatse Security. Excerpts from the chat logs are provided below.⁸

June 5, 2010

18. On or about June 5, 2010, defendant Spitler was chatting with "Nstyr" and "Pynchon," and the three considered the possible benefits of harvesting ICC-ID/e-mail pairings:

Spitler:	if you enter valid ICCIDs in this website you can get iPad subscriber email addresses I dont see the point unless we phish ⁹ for passes even then that's boring
Nstyr:	data minig *minig you could put them in a database for spamming for example sell them to spammers. . .
Spitler:	tru ipad focused spam
Pynchon:	harvest all the emails then expose it publicly

⁸ All spelling and grammatical errors throughout the IRC chats are per the original authors.

⁹ "Phishing" involves sending e-mails to users falsely claiming to be an established, legitimate enterprise in an attempt to scam the users into surrendering private information that will be used for identity theft.

Spitler: hahaha

Pynchon: tarnish at&t

Spitler: true

Nstyr: or sell if for thousands to the biggest spammers

19. Later that day, defendant Spitler reported the following to defendant Auernheimer:

Spitler: I just harvested 197 email addresses of iPad 3G subscribers there should be many more . . . weev: did you see my new project?

Auernheimer: no

Spitler: I'm stepping through iPad SIM ICCIDs to harvest email addresses if you use someones ICCID on the ipad service site it gives you their address

...

Auernheimer: loooool thats hilarious HILARIOUS oh man now this is big media news . . . is it scriptable? arent there SIM that spoof iccid?¹⁰

Spitler: I wrote a script to generate valid iccids and it loads the site and pulls an email

...

Auernheimer: this could be like, a future massive phishing operation serious like this is valuable data we have a list a potential complete list of AT&T iphone subscriber emails

Spitler: ipad but yeah

20. When defendant Spitler announced that he was "in a rut" and having difficulty determining additional ICC-ID/e-mail pairings, defendant Auernheimer assisted, offering: "SIM cards may be allocated by geographic region, either for number administration or network

¹⁰ "LOL" and its variants stand for laughing out loud.

planning reasons. The method of payment (pre-paid, post-paid) may be allocated on the SIM cards. . . . so sims are definitely preallocated either by geographic region sales channes, service providers or MVNOs question is who allocates them . . . probably AT&T suballocates free IDs to apple hopefully not at random . . . otherwise we have a real big space to search[.]”

21. On or about June 5, 2010, and again the following day, defendant Auernheimer encouraged defendant Spitler to amass as many ICC-ID/e-mail pairings as possible, writing: “if we can get a big dataset we could direct market ipad accessories[.]” Likewise, after learning that defendant Spitler had collected “625 emails,” defendant Auernheimer wrote: “takes like, millions to be profitable re: spam but thats a start[.]”

June 6, 2010

22. Responding to defendant Auernheimer’s encouragement, on or about June 6, 2010, defendant Spitler reported:

Spitler:	I hit fucking oil
Auernheimer:	looooool nice
Spitler:	If I can get a couple thousand out of this set where can we drop this for max lols?
Auernheimer:	dunno i would collect as much data as possible the minute its dropped, itll be fixed BUT valleywag i have all the gawker media people on my facecrook friends after goin to a gawker party

23. As defendant Spitler uncovered additional ICC-ID/e-mail pairings, he continued speaking with defendant Auernheimer about releasing the information to the press and, related, the legality of the data breach:

Spitler:	do I got to get involved
Auernheimer:	no
Spitler:	I’d like my anonaminity
Auernheimer:	alright
Spitler:	sry dunno how legal this is or if they could sue for damages
Auernheimer:	absolutely may be legal risk yeah, mostly civil you

absolutely could get sued to fuck

Spitler: D8¹¹

Auernheimer: alright i can wrangle the press just get me the codes and whatnot show me how to run this thing

24. Defendant Spitler then proceeded to provide the script to defendant Auernheimer, writing: “heres the script you run it php [script redacted] like first number is iccid minus the checkdigit second number is count or how many you want to check you have to pipe the output it just starts checking sequentially adding the proper checkdigit automatically lol[.]”

25. As defendants Spitler and Auernheimer were conversing, another Goatse Security member, “Rucas,” offered his advice on how best to use the ICC-ID/e-mail address pairings, stating: “dont go to the press sell the list to competitors . . . i just had an idea send out at&t phishing e-mails to all these idiots with an ipad trojan[.]”

26. As the data breach continued, defendant Auernheimer wrote to defendant Spitler: “if we get 1 reporters address with this somehow we instantly have a story . . . the best way to have a leadin on it . . . HI I STOLE YOUR EMAIL FROM AT&&T WANT TO KNOW HOW?” Defendant Spitler then proceeded to provide defendant Auernheimer with an ICC-ID and e-mail address for a member of the Board of Directors at News Corporation. Defendant Auernheimer sent an e-mail to that Board member, which read in relevant part:

An information leak on AT&T’s network allows severe privacy violations to iPad 3G users. Your iPad’s unique network identifier was pulled straight out of AT&T’s database We have collected many such identifiers for members of the media and major tech companies If a journalist in your organization would like to discuss this particular issue with us[,] I would be absolutely happy to describe the method of theft in more detail.

27. As the data breach continued, so too did the discussions between defendants Spitler and Auernheimer and other Goatse Security members about the best way to take advantage of the breach and associated theft:

Pynchon: hey, just an idea delay this outing for a couple days
tomorrow short some at&t stock then out them on tuesday
then fill your short and profit

Rucas: LOL

¹¹ The phrase “D8” means to be deeply involved in an activity or to perform an activity to the fullest extent possible.

Auernheimer: well i will say this it would be against the law . . . for ME to short the att stock but if you want to do it go nuts

Spitler: I dont have any money to invest in ATT

...

Auernheimer: if you short ATT dont let me know about it

Spitler: IM TAKIN YOU ALL DOWN WITH ME SNITCH HIGH EVERY DAY

June 7, 2010

28. After defendant Spitler announced that he had stolen over 100,000 ICC-ID/e-mail address pairings, defendant Auernheimer stated: "the more email addresses we get . . . the more of a freakout we can cause if nothing else we can pack these into a [database] . . . and do a mail merge and mail EVERYONE with an ipad 3g l o l[.]" To that, defendant Spitler responded simply: "lawlwla[.]"

June 9, 2010

29. After the Gawker Article was published, defendant Spitler was afflicted by "post-troll paranoia" and solicited advice from other Goatse Security members. "Rucas" offered the following: "what i'd do RIGHT NOW is open your router reset default passwords turn off wep etc that gives you some sort of plausible deniability that it was actually YOU using your internet if you can see other wireless networks in your area use their SSID that way idiots on xp will automatically connect to yours sometime and you can show that there are people who are NOT YOU on your network[.]"

30. Thereafter, the following conversation ensued:

Rucas: remember this key phrase

Spitler: again

Rucas: "I DON'T KNOW ANYTHING. I AM INVOKING MY MIRANDA RIGHT TO REMAIN SILENT."

Spitler: this Ian criminal isn't

Rucas: it is

Spitler: no

Rucas: why isn't it why don't you think it is

Spitler: cause I ddnt hack anything

Rucas: sure you did you did the exact same thing as changing a username in a url to gain access to a protected site

...

Rucas: you crossed state lines with ur packets so it's a federal crime

Spitler: tri tru

31. Later that day, defendants Spitler and Auernheimer and other Goatse Security members discussed who in the press had disclosed the data breach to AT&T, since, contrary to the Gawker Article, neither defendant nor anyone from Goatse Security had.¹² Indeed, defendant Auernheimer admitted as much to "Nstyr:"

Nstyr: you DID call tech support right?

Auernheimer: totally but not really

Nstyr: lol

Auernheimer: i dont fuckin care i hope they sue me

32. Related, the following conversation ensued:

Spitler: I bet [the publisher of the *San Francisco Chronicle*] leaked us to AT&T faggot is prob regretting not breaking the story acting like sf chron is a real paper still with integrity¹³

Jenk: lol

¹² The Gawker Article reported: "Goatse Security notified AT&T of the breach and the security hole was closed."

¹³ In addition to the e-mail sent to the Board member at News Corporation, defendant Auernheimer sent similar e-mails to the *San Francisco Chronicle* and Thomson-Reuters.

Spitler: or it wa all those reuters employees

...

Nstyr: you should've uploaded the list to full disclosure maybe you still can

Auernheimer: no no that is potentially criminal at this point we won

Nstyr: ah

Auernheimer: we dropepd the stock price

Nstyr: I guess

Auernheimer: lets not like do anything else we fucking win and i get to like spin us as a legitimate security organization

June 10, 2010

33. Fearful of the criminal repercussions of the data breach, defendants Spitler and Auernheimer had the following conversation during which they discussed destroying evidence of their crime:

Auernheimer: i would like get rid of your shit like are we gonna do anything else with this data?

Spitler: no should I toss it?

Auernheimer: i dont think so either might be best to toss

Spitler: yeah, I dont really give a fuck about it the troll is done

Auernheimer: yes we emerged victorious

Spitler: script is going byebye too

F. Losses

34. To date, AT&T has spent approximately \$73,000 in remedying the data breach. Those costs include, among other things, the cost of contacting all iPad 3G customers to inform them of the breach and AT&T's response to it.